(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－127197

(43)公開日　平成11年(1999)５月11日

(51)Int.Cl.[6]	識別記号	FI	
H04L 12/56		H04L 11/20	102D
G06F 13/00	353	G06F 13/00	353V
	355		355
H04L 12/18		H04L 11/18	

審査請求　未請求　請求項の数39　ＯＬ　外国語出願　（全 51 頁）

(21)出願番号　特願平10－184064

(22)出願日　平成10年(1998)６月30日

(31)優先権主張番号　０８／８８５８１７

(32)優先日　1997年６月30日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
SUN MICROSYSTEMS, INCORPORATED
アメリカ合衆国　94303　カリフォルニア州・パロ　アルト・サン　アントニオ　ロード・901

(72)発明者　アミット　グプタ
アメリカ合衆国、カリフォルニア　94040、マウンテン　ビュー　105、デル　メディオ　コート　2700

(74)代理人　弁理士　笹島　富二雄　（外１名）

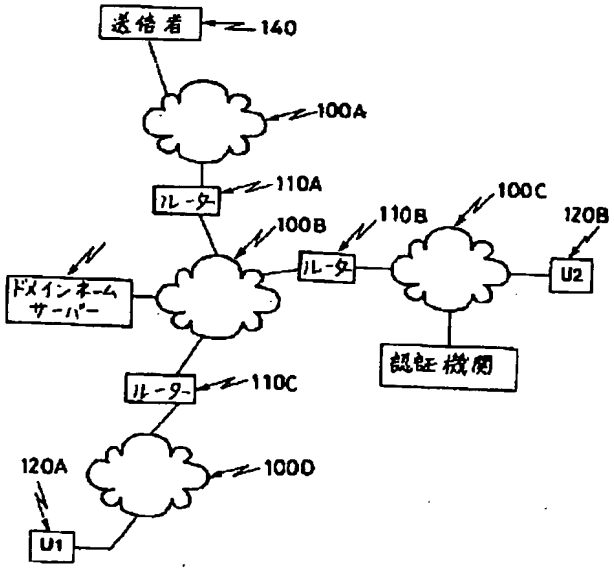
最終頁に続く

(54)【発明の名称】　インターネットマルチキャスティングにおけるデーターフローを保護するための技術

(57)【要約】　（修正有）

【課題】マルチキャスト通信が、プライベートマルチキャストの概念を含むように拡大される。

【解決手段】マルチキャスト専用のアドレス空間は、共用マルチキャスト用サブ空間と専用マルチキャスト用サブ空間とに区切られる。共用キー／専用キー暗号対が、専用マルチキャストに使用され、ドメインネームサーバー又は認証機関にインストールされる。マルチキャスト加入申請の部分は、対応する暗号化されたバージョンと共に送られる。専用マルチキャスト用ルーターは、マルチキャスト加入申請を受け取り、ドメインネームサーバー又は認証機関からの共用キーを検索し、申請者が認証されるべきか否かを決定するために、加入申請の暗号化された部分を解読する。グループ特定マルチキャスト加入は、マルチキャストに加入するユーザーへの送信を認証された送信者のグループか禁止された送信者のグループかを識別するビットマスクを送ることにより可能である。



1

【特許請求の範囲】

【請求項１】　少なくとも１つの入力ポートと、少なくとも１つの出力ポートと、入力ポートから出力ポートへのパケットのルーティングを制御する処理装置とを含んで構成されるマルチキャストデジタル通信用ルーティングエレメントであって、前記処理装置は、共用キーを獲得し、該共用キーを使用するユーザーにより提出されたマルチキャスト加入申請の少なくとも一部分を解読して、該ユーザーがマルチキャスト加入を認証されることを確認するように構成されることを特徴とするルーティングエレメント。

【請求項２】　前記共用キーは、ドメインネームサーバーから得られることを特徴とする請求項１記載のルーティングエレメント。

【請求項３】　前記共用キーは、認証機関から得られることを特徴とする請求項１記載のルーティングエレメント。

【請求項４】　前記ユーザーから提出されたマルチキャスト加入申請の解読が、前記ユーザーが特定のマルチキャストへの加入を認証されたことを示さない限り、前記特定のマルチキャストから前記ユーザーへのマルチキャストパケットをブロックすることを特徴とする請求項１記載のルーティングエレメント。

【請求項５】　前記処理装置は、マルチキャスト加入申請が専用マルチキャストアドレス空間内のマルチキャストアドレスを特定しているときにのみ、共用キーを獲得できるように構成されることを特徴とする請求項１記載のルーティングエレメント。

【請求項６】　前記処理装置は、マルチキャスト加入申請と共に受け取られるビットマスクにより示されるように、受信者への送信がブロックされている送信者から受け取ったマルチキャストパケットをブロックするように構成されることを特徴とする請求項１記載のルーティングエレメント。

【請求項７】　通信ポートと、前記通信ポートを経由した情報を制御する処理装置とを含んで構成されるマルチキャストに参加する装置であって、前記処理装置は、専用マルチキャスト加入申請を送信するように構成されることを特徴とする装置。

【請求項８】　前記マルチキャスト加入申請は、特定マルチキャストへの参加申請をするユーザーを識別するための第１フィールドと、前記第１フィールドの少なくとも１つ又は前記第１フィールドのダイジェストを専用キーを用いて暗号化した結果を有する第２フィールドと、を有することを特徴とする請求項７記載の装置。

【請求項９】　前記第２フィールドは、前記第１フィールドとランダムに作り出されたキー含む第３フィールドのうちの１つを暗号化した結果、又は前記第１フィールド及び前記第３フィールドのダイジェストを有することを特徴とする請求項７記載の装置。

2

【請求項１０】　前記加入申請は、少なくとも１つのビットマスクを含み、ビットマスクは、前記通信ポートへの送信を許可された送信者グループと前記送信ポートへの送信を禁止された送信者グループとを特定することを特徴とする請求項７の装置。

【請求項１１】　通信ポートと、共用／専用キー暗号対の対応する共用キーを使用してマルチキャスト用のネットワークアドレス又は別名に関する記録を記憶するメモリと、前記通信ポートを制御する処理装置と、を含んで構成されるドメインネームサーバーであって、前記処理装置は、前記通信ポートから受け取られたネットワークアドレス又は別名に応じて、前記対応する共用キーを送るように構成されることを特徴とするドメインネームサーバー。

【請求項１２】　前記記録は、マルチキャストの所有者の表示を含むことを特徴とする請求項１１記載のサーバー。

【請求項１３】　前記記録は、マルチキャストが共有であるか専用であるかを識別するための表示を含むことを特徴とする請求項１１記載のサーバー。

【請求項１４】　少なくとも１つのソースから複数の受信者への情報をマルチキャストするための通信システムであって、各々がそれ自体に接続された少なくとも１つのユーザー装置を有する複数のサブネットワークと、少なくとも２つのサブネットワークと接続し、共用マルチキャストと専用マルチキャストとを識別するように構成される少なくとも１つのルーティングエレメントと、を含んで構成されることを特徴とする通信システム。

【請求項１５】　さらに、サブネットワークに接続されて、専用／共用キー暗号対の共用キーでネットワークアドレス又は別名に関する記録を記憶するドメインネームサーバーを含んで構成されることを特徴とする請求項１４記載のシステム。

【請求項１６】　さらに、サブネットワークに接続されて、共用／専用キー暗号対の共用キーでネットワークアドレス又は別名に関する記録を記憶する認証機関を含んで構成されることを特徴とする請求項１４記載のシステム。

【請求項１７】　ユーザー装置は、専用マルチキャストへの参加を申請するように構成されることを特徴とする請求項１４記載のシステム。

【請求項１８】　共用マルチキャスト用サブ空間と専用マルチキャスト用サブ空間とを有するマルチキャストアドレス空間を提供するステップを含んで構成されることを特徴とする通信システムを操作する方法。

【請求項１９】　ユーザーの識別を含む第１の情報を、前記第１の情報の暗号化されたバージョンとともに送るステップを含んで構成されることを特徴とするマルチキャスト加入申請を送信する方法。

【請求項２０】　前記第１の情報は、さらに任意のキー

を含むことを特徴とする請求項１８記載の方法。

【請求項２１】　ユーザーからのマルチキャスト加入申請を送信する方法であって、前記ユーザーに送信することを許可された送信者のグループと前記ユーザーに送信することを禁止された送信者のグループの少なくとも１つを特定するビットマスクのリストを送信するステップを含むことを特徴とする方法。

【請求項２２】ルーターでマルチキャスト加入申請を処理する方法であって、前記申請が共用マルチキャストか又は専用マルチキャストかを決定する方法。

【請求項２３】　さらに、共用キーを獲得し、前記共用キーを使用して前記申請の少なくとも一部分を解読するステップを含んで構成されることを特徴とする請求項２１記載の方法。

【請求項２４】　さらに、前記申請の解読された部分が前記申請の他の部分に一致したとき、前記申請を許可するステップを含んで構成されることを特徴とする請求項２２記載の方法。

【請求項２５】　共用／専用キー暗号対を作成するステップと、マルチキャストの認証された参加者に専用キーを分配するステップと、専用マルチキャストアドレスを獲得するステップと、マルチキャスト用共用キーをドメインネームサーバー又は認証機関にインストールするステップと、を含んで構成されることを特徴とする専用マルチキャストを設立する方法。

【請求項２６】　メモリ媒体と、前記メモリ媒体に記憶されたコンピュータプログラムと、を含んで構成されるコンピュータプログラム製品であって、前記コンピュータプログラムは、共用マルチキャスト用サブ空間と専用マルチキャスト用サブ空間とを有するマルチキャストアドレス空間を提供するための命令を含むことを特徴とするコンピューターープログラム製品。

【請求項２７】　前記プログラムは、前記メモリ媒体から、ネットワークインタフェースを通って伝送されることを特徴とする請求項２５記載のコンピューターープログラム製品。

【請求項２８】　メモリ媒体と、前記メモリ媒体に記憶されたコンピュータプログラムと、を含んで構成されるコンピュータプログラム製品であって、前記コンピュータプログラムは、前記ユーザー識別の暗号化されたバージョンと共に、ユーザー識別を含むマルチキャスト加入申請を送るための命令を含んで構成されることを特徴とするコンピュータプログラム製品。

【請求項２９】　前記プログラムは、前記メモリ媒体から、ネットワークインタフェースを通って伝送されることを特徴とする請求項２７記載のコンピュータプログラム製品。

【請求項３０】　メモリ媒体と、前記メモリ媒体に記憶されたコンピュータプログラムと、を含んで構成されるコンピュータプログラム製品であって、前記コンピュータプログラムは、前記ユーザーへの送信を許可された送信者のグループと前記ユーザーへの送信を禁止された送信者のグループの少なくとも１つを特定するビットマスクを含むグループ特定マルチキャスト加入を送るための命令を含んで構成されることを特徴とするコンピュータプログラム製品。

【請求項３１】　前記プログラムは、前記メモリ媒体から、ネットワークインタフェースを通って伝送されることを特徴とする請求項２９記載のコンピュータプログラム製品。

【請求項３２】　メモリ媒体と、前記メモリ媒体に記憶されたコンピュータプログラムと、を含んで構成されたコンピュータプログラム製品であって、前記コンピュータプログラムは、申請が共用マルチキャストに関するものであるか、専用マルチキャストに関するものであるかを決定し、専用キーを獲得して、共用キーを使用して前記申請の少なくとも一部分を解読するための命令を含んで構成されることを特徴とするコンピュータプログラム製品。

【請求項３３】　前記プログラムは、前記メモリ媒体からコンピュータインタフェースを通って伝送されることを特徴とする請求項３１記載のコンピュータプログラム製品

【請求項３４】　メモリ媒体と、前記メモリ媒体に記憶されたコンピュータプログラムと、を含んで構成されるコンピュータプログラム製品であって、前記コンピュータプログラムは、専用／共用キー暗号対を作成し、専用マルチキャストアドレスを獲得し、マルチキャスト用の共用キーをドメインネームサーバー又は認証機関にインストールする命令を含んで構成されることを特徴とするコンピュータプログラム製品。

【請求項３５】　前記プログラムは、前記メモリ媒体からネットワークインタフェースを通って伝送されることを特徴とする請求項３３記載のコンピューターープログラム製品。

【請求項３６】　搬送波に包含され、一連の命令を表すコンピュータデータ信号であって、上記一連の命令は、１以上の処理装置によって実行されたとき、上記１以上の処理装置に、共用キーを獲得させ、前記共用キーを用いてユーザーから提出されたマルチキャスト加入申請の少なくとも一部分を解読させることを特徴とするコンピュータデータ信号。

【請求項３７】　メモリに記憶されたデータ構造を含んで構成され、コンピュータ上で実行されるアプリケーションプラグラムによるアクセスのためのデータを記憶するメモリであって、前記データ構造は、ＩＧＭＰ加入申請と、申請者のＩＰアドレスと、前記ＩＰＧＭ加入申請と前記申請者のＩＰアドレストに含まれる情報の少なくとも一部の暗号化バージョンと、を含んで構成されることを特徴とするメモリ。

【請求項３８】　メモリに記憶されたデータ構造を含んで構成され、コンピュータ上で実行されるサーバープログラムによるアクセスのためのデータを記憶するメモリであって、前記データ構造は、複数のエントリーを含み、各エントリーはマルチキャストアドレスと、前記マルチキャストアドレスが共用マルチキャストであるか専用マルチキャストであるかの指示と、を含むことを特徴とするメモリ。

【請求項３９】　前記データ構造のエントリーは、共用キーの記憶位置を含むことを特徴とする請求項３８記載のメモリ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は通信システム、特にインターネットマルチキャスティングにおけるデータフローの保護に関する。

【０００２】

【従来の技術】従来の多くのインターネットアプリケーションは、一人対多数、多数対多数の通信を含み、この場合、１つ又は多数のソースから多数の受信者に送信される。例として、従業員への社内メッセージの送信、ブローカーへの株式相場連絡、遠隔地ミーティング用及び遠距離通勤用ビデオ及びオーディオ会議、データベース及びウェブサイト情報の複写がある。ＩＰマルチキャストは、ソースが単一のメッセージコピーをメッセージの受信を欲する多数の受信者に送れるようにすることで、このタイプの送信を効果的に支援する。これは、ソースが、メッセージのコピーを個別に各要求者に送る（ポイントーポイントユニキャストと呼ばれる）必要がある場合よりもはるかに効果的であるが、このような場合、送信者に利用可能な帯域幅によって受信者の数が制限される。また、多くのノードはメッセージを必要とせず、又は放送は単一のサブネットに限定されているので、ネットワークの全てのノード（放送）にメッセージの１つのコピーを送るよりも、はるかに効果的である。

【０００３】ＩＰマルチキャスティングは受信者ベース概念であり、受信者が特定マルチキャストセッショングループに加入すると、ネットワーク基盤によってグループのすべてのメンバーとの交流が行われる。送信者は、受信者のリストを保持する必要がない。マルチキャストメッセージのただ１つのコピーが、ネットワークのどんなリンクも通過し、メッセージの複数のコピーが、ルーターでパスが分岐する場合にのみ作られる。このように、マルチキャストは多大の実行の改良を生み出し、周波数帯域幅端部から端部を保護する。

【０００４】ＩＰマルチキャスティングは、ＩＰマルチキャストイニシアティブによって、発表された２つの論文に、より詳細に述べられている。その一つは、「How IP Multicast Works」で、他の一つは、「Introduction to IP Multicast Routing」という表題である。ここでは、これらの論文の大部分を先行技術として本明細書に組み込んでいる。

【０００５】データストリームの暗号化を使用するマルチキャストの保護方法は、公知であり、送信者が、受信者側での解読のための出力情報を暗号化するものである。これは、一般的に、共用キー暗号化技術を使用してなされる。

【０００６】

【発明が解決しようとする課題】ＩＰマルチキャスティングは、送信者が、単に、マルチキャストグループアドレスにデーターを送り、該アドレス上のデータを受け取ることに対する興味を明示したあらゆる人にネットワークが自動的にそのデータを送るという、簡単な設計に基づくものである。しかし、この方法では、データーフローに対するいかなる保護も提供されていないこと、即ち、誰でもマルチキャストセッションを受信できるとともに、マルチキャストセッションにデータを送ることができることが重要な問題点である。結果として、従来技術では、インターネットマルチキャスティングセッションにおいて、安全なデータフローのようなものがない。さらに、だれもがマルチキャストセッションに送信することができるので、侵入者による破壊の可能性が大きい。

【０００７】

【課題を解決するための手段】ここに記載の発明の種々の態様は、インターネットマルチキャスティングにおけるデータ流れの保護のための装置、システム、方法、コンピュータープログラム製品を提供する。これは、マルチキャストアドレス空間を、１つは共用マルチキャスト用と、１つは専用マルチキャスト用と、の２つの構成要素に分割することにより達成される。共用／専用対の共用キーは、ドメインネームサーバー又は認証機関にインストールされ、マルチキャストアドレスと、関連する。専用マルチキャストに加入を希望するユーザーは、共用／専用キー対の専用キーを用いて暗号化された一定情報を提供する。ルーティング機能は、一般的には、スイッチングネットワークのノードによるスイッチ、又はネットワークのルーター、又は複数の通信インタフェースを持つコンピュータにより実行される。ここで使用されるように、「ルーティングエレメント」という語句は、すべてに適用される。ルーティングエレメントは、加入申請を受信し、共用キーを獲得して、任意の暗号化されない情報と解読された情報との一致性について比較する。ルーティングエレメントは、受領した加入申請の他の一定の検査も行う。受領した加入申請が信頼できることをルーティングエレメントが認めたときのみ、ルーティングエレメントは加入を許可しソースへの途中にある次のルーティングエレメントに加入申請を送る。技術は、ソースグループの特定の加入脱退に対応するもので、これは受信者にデータを送ることが認証された送信者を特定

させ、認証されていない送信者が受信者にデータを送ることを防止させる。

【０００８】本発明の１つの実施形態は、マルチキャスト情報のためのルーティングエレメントに関する。ルーティングエレメントは共用キーを獲得し、これを用いてマルチキャスト加入申請の一部を解読して、ユーザーが専用マルチキャストへの加入を認証されていることを確認する。本発明の他の実施形態は、専用マルチキャスト加入申請を送るように構成された処理装置を含むマルチキャストに参加する装置に関する。

【０００９】本発明の他の実施形態は、マルチキャストネットワークアドレスまたは別名に関する記録を共用／専用キーの暗号対の共用キーを用いて記憶し、通信ポートを介して受信したネットワークアドレス又は別名に応答してアドレス又は別名に対応する共用キーを送るドメインネームサーバーに関する。本発明の他の実施形態は、複数のサブネットワークと、少なくとも1 つのルーターとを有し、少なくとも2 つのサブネットワークを接続し、共用マルチキャストか専用マルチキャストかを識別するように構成された、少なくとも1 つのソースから複数の受信者に情報をマチキャストする通信システムに関する。

【００１０】本発明の他の実施形態は、共用マルチキャスト用サブ空間と専用マルチキャスト用サブ空間とを有するマルチキャストアドレス空間を提供することによって、通信システムを処理する方法に関する。本発明の他の実施形態は、ユーザー識別と任意のランダムキーとを含む第１の情報を、前記第１の情報の暗号化されたバージョンと共に送ることにより、マルチキャスト加入申請を送信する方法に関する。

【００１１】本発明の他の実施形態は、使用者に送信することを許可された送信者グループと、使用者に送信することを禁止された送信者グループの少なくとも１つを特定するビットマスクのリストと、を送ることにより、ユーザーからのマルチキャスト加入申請を送信する方法に関する。本発明の他の実施形態は、専用／共用キー暗号対を作成し、マルチキャスト内の認証された参加者に専用キーを分配し、専用マルチキャストアドレスを獲得し、ドメインメームサーバー又は認証機関にマルチキャスト用専用キーをインストールすることによる専用マルチキャストの設立方法に関する。

【００１２】本発明の他の実施形態は、上記の技術を実行するためのコンピュータプログラム製品に関する。本発明の上記の及びその他の特徴、態様、利点は、添付の図面を参照して、以下に記載する本発明の詳細な説明により、より明白になるであろう。本発明のシステムの目的、特徴、利点は、以下の記載により明らかになる。

【００１３】

【発明の実施の形態】記号及び、学術用語以下の詳細な説明は、コンピューターやコンピューターネットワーク上で実行されるプログラム処理に関して提示される。これらの処理の記載と表現は、当業者により使用される手段であって、その研究の実体を他の当業者に最も効果的に伝達するためのものである。

【００１４】処理とは、ここでは一般的に、所望の結果を導く筋道だった一連のステップと考えられる。これらのステップは、物理的量の物理的操作を必要とするものである。通常は、必ずしも必要というわけではないが、これらの量は、記憶、伝達、結合、比較、操作が可能な電気信号又は磁気信号の形状をとっている。これらの信号をビット、値、要素、記号、文字、言語、数字等と呼ぶことは、主として共通使用の理由から、時として便利である。しかし、これらの及びこれらに類似する語句のすべては、適宜な物理的量と関連するものであり、単に、これらの量に付けられる便宜上のラベルであることは言うまでもない。

【００１５】さらに、実行される操作は、しばしば加える、比較する等の言語で呼ばれ、これらは、オペレーターによって実行される精神的操作に共通に関連する。ここに記載の本発明の一部を構成する操作のいずれにおいても、多くの場合、オペレーターにさほどの能力を必要せず、或いは要求もされない。これらの操作は、機械操作である。本発明の操作を実行するための有用な機器には、汎用デジタルコンピューターやそれに類する装置が含まれる。

【００１６】本発明は又、これらの操作を実行するための装置に関する。この装置は、必要な目的のために特に構成されてもよいし、あるいは、コンピューターに記憶されているコンピュータープログラムによって選択的に起動し、再構成されるような汎用コンピューターを含んで構成されてもよい。ここで提供される処理は、特別なコンピューターやその他の装置に本質的に関するものではない。種々の汎用機器が、本発明の技術に従って書き込まれたプログラムを用いて使用できる。また、必要な方法ステップを実行するためのより特定の装置を構築するのにより便利であることを証明する。これらの種々の機器のための必要な構成が本発明から明らかになる。

【００１７】図１は、本発明の１つの態様によれば、複数のサブネットワークをリンクするネットワーク配列の一例を示すブロック図である。図１に示すように複数のサブネットワーク１００Ａ，１００Ｂ，１００Ｃ，１００Ｄがルーター１１０Ａ，１１０Ｂ，１１０Ｃを介して相互に接続されている。図示されるネットワークでは、ドメインネームサーバー１３０は、サブネットワーク１００Ｂ上に常駐し、認証サーバー又は認証機関１５０は、サブネットワーク１００Ｃ上に常駐する。１以上の送信者１４０は、ユーザーステーション１２０Ａ，１２０Ｂなどに対するマルチキャストを目的とする情報源である。

【００１８】図２は、マルチキャストアドレス空間が、

どのように専用マルチキャストアドレスサブ空間と共用マルチキャストアドレスサブ空間とに区分されているかを示す。図２の左側にはマルチキャストアドレス空間全体が表示されている。この空間は２２４．０．０．０から２３９．２５５．２５５．２５５（インターネット標準によるドット十進表示）の範囲である。ドット十進表示の下側には、ドット十進表示の最初の要素の数値に相当する８個のビット（括弧内）が挿入的に表示されている。ドット十進表示の他の要素の各々は、インターネットで使用されている３２ビット（４バイト）アドレス空間内の対応するバイトの数値を表示する。同じ二進数値の別の表示からドットにより区切られた二進数値の１又は０の表示は、３２－ビットアドレスワードの残りのビットが、その内部に含まれる二進数値のみを有するという指示を表している。本発明により提供されるマルチキャストアドレス空間の拡大における重要点の１つは、マルチキャストアドレス空間を一方を共用マルチキャストアドレス空間、他方を専用マルチキャストアドレス空間の２つの構成部分に分割することである。図２に示すように、共用マルチキャストアドレス空間は、２２４．０．０．０から２３１．２５５．２５５．２５５までの範囲である。同様に、専用マルチキャストアドレス空間は、２３２．０．０．０から２３９．２５５．２５５．２５５までの範囲である。このアドレス空間の分割により、専用マルチキャストが行われるか、共用マルチキャストが行われるかをマルチキャストアドレスから即座に知ることができる。

【００１９】図３は、先行技術における典型的なドメインネームサーバー（ＤＮＳ）記録を示すデータベーススキーマである。図３に示すように、ドット十進アドレス３００は、データベース表の各欄のドット十進アドレス３１０の別名に対してマップされる。図４は、本発明の１つの態様により修正を加えたドメインネームサーバーのデータベーススキーマである。欄４００、４１０は、図３のエントリ３００、３１０が発生する欄にほぼ対応する。しかし、４１０の欄には、固定ステーションアドレスの代わりに、ＩＰマルチキャストアドレスが含まれる。欄４２０は、マルチキャストアドレスの所有者を記述するエントリを含む。一般的には、これは、マルチキャストを設定した者である。欄４３０は、各専用マルチキャストのための共用キーを含む。欄４４０は、アドレス空間が分割されていない場合に、共用マルチキャストか専用マルチキャストかを識別するのに使用できる任意の共用又は専用フラグを含む。

【００２０】従来技術のドメインネームサーバーを使用した場合は、ネットワークアドレス又はその別名のいずれかを使用する照会により図３に示される他方の数値が返却される結果となる。ドメインネームサーバーが、図４に示す配置に従って拡張された場合、欄４００又は欄４１０のいずれか一方からのデータを用いて提出される照会により、提出された数値に適合した記録全体が返却される結果となることは便利である。このように、図４の欄４１０に示される別名を検索すると、欄４００に示されるネットワークアドレスと欄４２０に示される所有者情報だけではなく、マルチキャスト会議のための欄４３０に示される共用キーも検索することになる。以下に詳細に説明するように、共用キーを検索するためのこの能力は有用である。

【００２１】図５は、本発明の一態様による、インターネット組合管理プロトコル（ＩＧＭＰ）加入申請への拡張を示す図である。ヘッダ５００と、フィールド２に示される申請者のＩＰアドレスの申請者と共にフィールド１に示されるパケットタイプとは、一般に従来のＩＧＰＭＰ加入申請の一部である。本発明の態様にしたがって示される拡張において、任意のタイムスタンプが、フィールド１に配置でき、フィールド３に配置されるランダムキーは申請者によって作成される。フィールド１，フィールド２，フィールド３の内容は暗号化又は分類され、そのダイジェストは暗号化され、フィールド４に配置される。巡回冗長検査（ＣＲＣ）は、ＩＧＭＰ加入申請全体に行う。この拡張された加入申請の実用化の方法を以下に詳細に説明する。

【００２２】図６は、本発明の一態様による、ＩＧＭＰ加入申請を許可するか拒絶するかを判定するためのルーティングエレメントの処理の一例を示すフローチャートである。拡張されたＩＧＭＰ加入申請がルーター６００で受領されると、マルチキャストが共用であるか専用であるかをアドレスから決定する（６０５）。共用の場合（６０５において共用を判定）加入が許可され、加入申請は、もしあれば、パスに沿って次のルーティングエレメントに送られる（６４０）。マルチキャストが専用の場合は（６０５において専用を判定）、提出された加入申請が以前に提出された申請の複写であるか否かの判定をするためのチェックが行われる。認証されていないユーザーが、マルチキャストへのアクセス権を得るために企てる方法として、以前のユーザーが提出した加入申請を複写することがあげられる。提出された加入申請が複写の場合、（６１０においてＹＥＳ）申請は拒絶される。複写でない場合、加入申請が期間内であるか否かの判定がなされる（６１５）。これは、その加入申請が、現在のマルチキャストセッションの日時に適合しているか否かを調べる簡単な検査である。これにより、ユーザーが、認証されたユーザにより以前に提出された加入申請を複写して、現在のマルチキャストセッションへのアクセス権を獲得しようとする企てを防止できる。加入申請が、期間内のものでない場合（６１５においてＮＯ）、その申請は拒絶される。もし、期間内であれば、その加入申請が正当なリンクからきたものか否かを判定するための検査を行う。もし、正当なリンクからのものでない場合は（６２０においてＮＯ）、その加入申請は

拒絶される。しかし、正当なリンクからのものであれば、ルーティングエレメントは、ＩＧＭＰの拡張された加入申請を暗号化するのに使用される専用キーに対応する二重の共用キーを獲得する（６２５）。共用キーは、図１に示すＤＮＳ１３０のようなドメインネームサーバーから得るのが望ましい。或いは、図１に示す認証機関１５０から得ることもできる。獲得した共用キーを使用して、拡張されたＩＧＭＰ加入申請のフィールド４は、その共用キーを使って解読される（６３０）。フィールド４から解読された結果としての情報は、フィールド１－３に一致する必要がある。一致すれば加入申請は認められ、その加入申請は次のルーティングエレメントに送られる。一致しない場合（６３５においてＮＯ）、加入申請は拒絶され、ルーターによりそのユーザーのマルチキャストへのアクセス権が否認される。

【００２３】本発明の第三の態様を、図７Ａ、図７Ｂ，図７Ｃに示す。図７Ａは、従来のＩＧＭＰ加入申請を示す。図７Ｂは、図７ＡのＩＧＭＰ加入申請への従来の拡張を示す。図７ＢのＩＧＭＰ加入申請の拡張により、加入を申請するアドレスに送信することを許可された送信者のリストが特定される。同様に、これは、加入を申請するアドレスへの送信を禁止された送信者のリストも含む。これにより、マルチキャストの参加者は、望ましくない若しくは破壊的なソースからのパケットが参加者に届かないように選択的に禁止することをルーターに通知することができる。これはまた、要求するステーションが情報を受け取ることを希望する送信者のリストをユーザーが特定できるようにするものである。これにより、ユーザーが見たくないパケットを取り除くことができる。

【００２４】図７Ｃは、本発明の一態様による、従来のＩＧＭＰ加入申請の拡張を示す。フィールド７６０、フィールド７７０は、送信者又は受信者のリストに代えて、３２ビットマスクのリストの使用を認める。このように、マスクを作ることによって、アドレスグループ及び所望の特性にふさわしいビットマスクを特定するだけで、アドレスグループを、そのアドレスに送ることを許可し、或いは禁止することができる。たとえば、特性は「このアドレスに送信するとが許可される」、又は「このアドレスに送信することが禁止される」であってよい。

【００２５】図８は、本発明の一態様による、専用マルチキャストを設立するための処理を示すフローチャートである。専用マルチキャストの設立を所望するユーザーは、まず、マルチキャスト用の専用／共用キーの対を作成する（８００）。マルチキャストの提供者または所有者は、マルチキャスト中に使用するための専用マルチキャストアドレス（８１０）を獲得する。これは、継続的な仕事であっても、必要に応じた一時的な仕事であってもよい。マルチキャストの所有者又は他の指定されたパーティーは、マルチキャストアドレスのためのドメインネームサーバー情報、又は認証機関にマルチキャスト用共用キーをインストールする（８２０）。マルチキャスト用専用キーは、いくつかの公知の方法のうちのいずれかにより、認証された参加者に提供されるが、ネットワークを通じるのが好ましい（８１０）。この時点で、マルチキャストを開始できる（８４０）。そして、マルチキャストへの参加を所望する受信者は、図５に示すような拡張型加入申請を作成する。使用者が認証されると、ルーティングエレメントは、ドメインネームサーバーまたは認証機関にインストールされている共用キーの使用を決定する。ルーティングエレメントは、専用マルチキャストへの加入申請が本物であることを確認すると、拡張型ＩＧＭＰ加入申請で提出されたユーザーに、マルチキャストアドレスにアドレスされたパケットを送り始める。もし、利用者が認証されない場合（図６に関連して述べられているように）、ユーザーは、マルチキャストに加入することを許可されず、ルーティングエレメントは、ユーザーにパケットを送らない。

【００２６】図９Ａは、本発明を実施するのに適したタイプのコンピュータを示す。図９Ａを外側から見ると、コンピュータシステムは、ディスクドライブ９１０Ａ、９１０Ｂを有する中央処理装置９００を有している。ディスクドライブ表示９１０Ａ，９１０Ｂは、このコンピュータシステムに収容される多数ののディスクドライブの単なる符号である。概して、これらには９１０Ａのようなフロッピーディスクドライブ、ハードディスクドライブ（外部からは示されていない）、スロット９１０Ｂで示されるＣＤ－ＲＯＭドライブが含まれる。概して、ドライブの数と種類は、種々のコンピュータ構造に応じて変化する。コンピュータは、情報を表示するディスプレイ９２０を有する。キーボード９３０とマウス９４０も又一般に、入力装置として利用できる。図９Ａに示すコンピュータは、サンマイクロシステムズインコーポレーテッドのＳＰＡＲＣワークステーションであるのが好ましい。

【００２７】図９Ｂは、図９Ａのコンピュータの内部ハードウエアのブロック図を示す。バス９５５は、コンピューターの他の構成部分を相互に接続する主要な情報の幹線路としての役目を果たす。ＣＰＵ９５５は、本システムの中央処理装置で、プログラムの実行に必要な計算と論理演算とを行う。読み出し専用メモリ９６０とランダムアクセスメモリ９６５とが、コンピュータの主メモリを構成する。ディスクコントローラ９７０は、システムバス９５０に１以上のディスクドライブをインタフェースする。これらのディスクドライブは、９７３のようなフロッピードライブ、９７２のような内部若しくは外部ハードドライブ、又は、９７１のようなＣＤ－ＲＯＭドライブやＤＶＤ（デジタルビデオディスク）ドライブでよい。ディスプレイインタフェース９２５は、ディス

プレイ９２０とインタフェースし、バスからの情報をディスプレイ上で見られるようにする。外部装置との通信は、通信ポート９８５を介して実行できる。

【００２８】コンピューター９００は、バス９５０に接続された通信インタフェース９８５を有する。通信インタフェース９８５は、図１の１００Ｄのようなローカルネットワークへのネットワークリンクとの双方向データ通信接続を提供する。たとえば、通信インターフェイス９８５がサービス統合デジタル網（ＩＳＤＮ）カード又はモデムの場合、通信インターフェイス９８５は対応するタイプの電話線とのデーター通信接続を提供する。通信インタフェース９８５がローカルエリアネットワーク（ＬＡＮ）の場合、通信インタフェース９８５はコンパチブルＬＡＮへのデータ通信接続を提供する。無線リンクも又可能ある。このような配置のいずれにおいても、通信インタフェースは９８５は、種々のタイプの情報を表すデジタルデーターストリームを保持する電気信号、電磁信号，若しくは光信号を送受信する。

【００２９】ネットワークリンクは、一般的には、図１の１００Ａ－１００Ｄのような１以上のネットワークを介してデータ通信を他のデータ装置に提供する。たとえば、ネットワークリンクが、ローカルネットワークを介して、ホストコンピュータとの接続、又はインターネットサービスプロバイダー（ＩＳＰ）によって操作されるデータ装置との接続を提供する。ＩＳＰは、現在、一般的にはインターネットといわれる世界規模のパケットデータ通信ネットワークを介して、次々にデータ通信サービスを提供する。ローカルネットワークとインターネットは、共にデジタルデータストリームを保持する電気信号、電磁信号、光信号を使用する。種々のネットワークを介した信号とネットワークリンク上や通信インタフェース９８５を介した信号とは、コンピュータ９００のデジタルデータ及びコンピュータ９００からのデジタルデータを保持するものであるが、情報を伝達する搬送波形状を示す。

【００３０】コンピュータ９００は、ネットワーク、ネットワークリンク及び通信インタフェース９８５を介して、メッセージを送信し、プログラムコードを含むデータを受信する。インターネットの場合には、サーバーは、アプリケーションプログラム用コードをインターネット、ＩＳＰ、ローカルネットワーク及び通信インタフェース９８５を介して送信できる。本発明によれば、ダウンロードアプリケーションのようなものが、ここに記載の技術を実行するソフトウエアを含む。

【００３１】受信されたコードは、受信されたときに、処理装置９５５で実行され、及び／又は後の実行のために記憶装置９６０及び／又は９７１－９７３、又は他の不揮発性記憶装置に記憶される。このように、コンピュータ９００は、搬送波形状のアプリケーションコードを獲得できる。図９は、ユーザーワークステーション又はルーティングエレメントに適したアーキテクチャを示す。しかし、ルーティングエレメントとして構成された場合、Ｉ／Ｏ装置は、通常はサービスの間だけ取り付けられていればよい。ルーターとして構成された場合、通常は、複数の通信インタフェース９８５が各ポートに１つ提供される。スイッチングノードにおけるスィッチ用コントローラとして構成された場合、ハードウエアインタフェースは、スイッチングマトリックスにバス９５０をリンクするために提供される。

【００３２】図９Ｃは、図９Ｂの９７３又は図９Ａの９１０Ａのような装置で使用される記憶媒体の例を示す。一般的には、フロッピードライブ、ＣＤ－ＲＯＭ、デジタルビデオディスクのような記憶媒体が、コンピュータを制御するためのプログラム情報を含んで、コンピュータが本発明に従ってその機能を実行できるようにする。

【００３３】上記方法は、多様なユーザーのニーズの範囲にわたって作動する簡単な汎用性のあるインタフェースを提供する。これは、簡単なオープン会議を設立し続けたいユーザーのためのマルチキャストを設立し操作するための経費を不合理に増大させるものではない。部外者がＩＰアドレス及び／又はポート番号を知って、誤作動させ若しくは故意により作動させる可能性がある場合であっても、本システムはセキュリティを提供する。マルチキャストセッションの構成員が事前にすべての送信者及び／又は聴衆の身分を知る必要がない点において、本システムは適用性がある。本システムは、又、ユーザーの会議への積極的な参加を可能にする。

【００３４】本システムが悪化したとしても、そのユーザーまたはユーザーのグループを会議から排除することによる損害を合理的に最小限とすることができる。ここに記載の方法は、また、現在及び将来のマルチキャスト用メカニズムとプロトコルに合致する。本発明を、詳細に説明してきたが、本発明は、図面や実施例のみで解釈されるが、これに限定されるべきではなく、本発明の精神及び範囲は、添付の特許請求の範囲及びその均等物によってのみ限定されることが明らかに理解される。

【００３５】

【図面の簡単な説明】

【００３６】

【図１】　本発明の一態様による、複数のサブネットワークをリンクするネットワークの一例を示すブロック図。

【００３７】

【図２】　本発明の一態様による、マルチキャストアドレス空間が、いかに専用マルチキャストアドレスサブ空間と共用マルチキャストアドレスサブ空間とに区切られているかを示す図。

【００３８】

【図３】　従来技術による、一般的なドメインネームサ

15

ーバーレコードのデータベーススキーマを示す図。

【００３９】

【図４】　本発明の一態様による、修正されたドメインネームサーバーのデータベーススキーマを示す図。

【００４０】

【図５】　本発明の一態様による、インターネットグループ管理プロトコル（ＩＧＭＰ）加入申請への拡張を示す図。

【００４１】

【図６】　本発明の一態様による、ＩＧＭＰ加入申請を許可するか、拒絶するかを決定するためのルーター処理の一例を示すフローチャート。

【００４２】

16

【図７】　Ａは、従来のＩＧＭＰ加入申請を示す図であり、Ｂは、図７ＡのＩＧＭＰ加入申請への従来の拡張を示す図であり、Ｃは、本発明の一態様による、ＩＧＰＭ加入申請への拡張を示す図である。

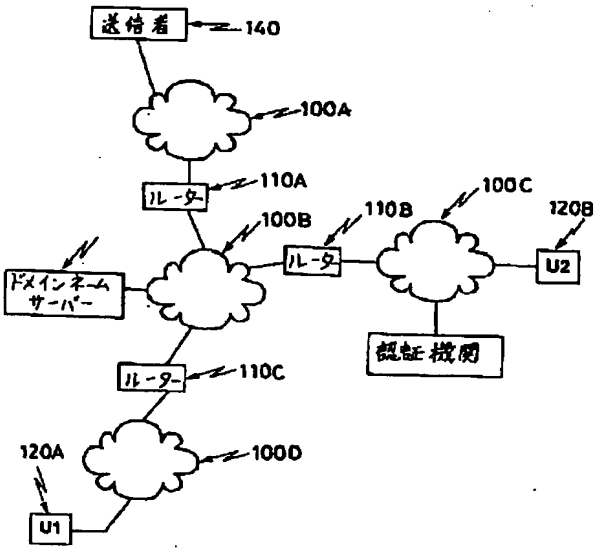
【００４３】

【図８】　本発明の一態様による、専用マルチキャスト設立のための処理を示すフローチャート。

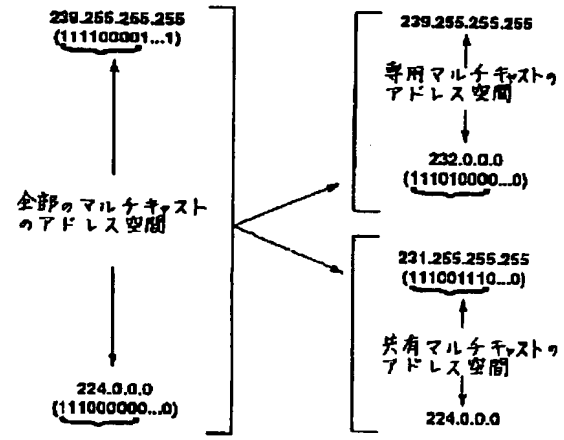
【００４４】

【図９】　Ａは、本発明を実施するのに適したタイプのコンピューターを示す図であり、Ｂは、図９Ａのコンピューターのブロック図であり、Ｃは、図９Ａのコンピューターで使用可能な１以上のプログラムを含む記録媒体の例を示す図である。

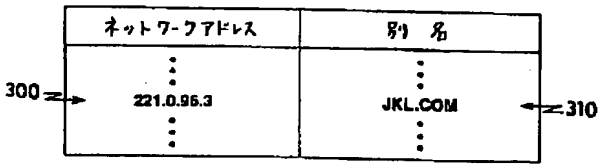
【図１】



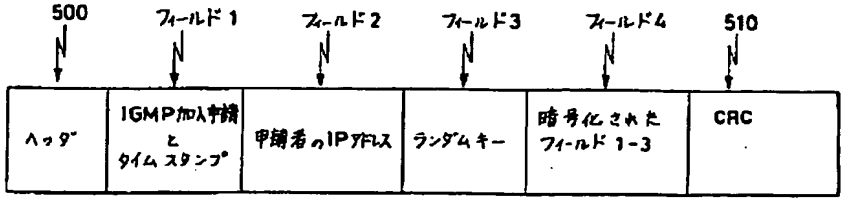
【図２】



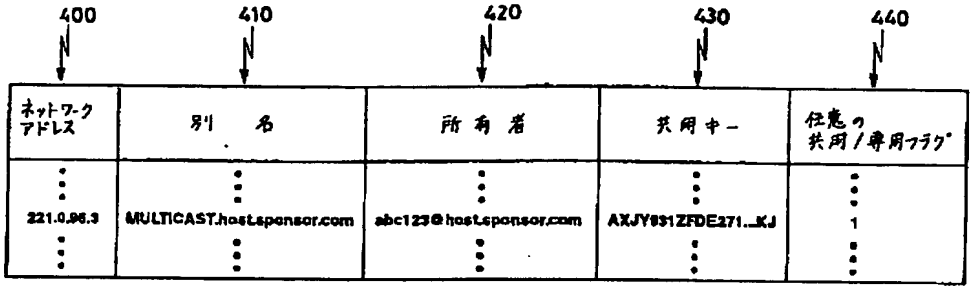
【図３】



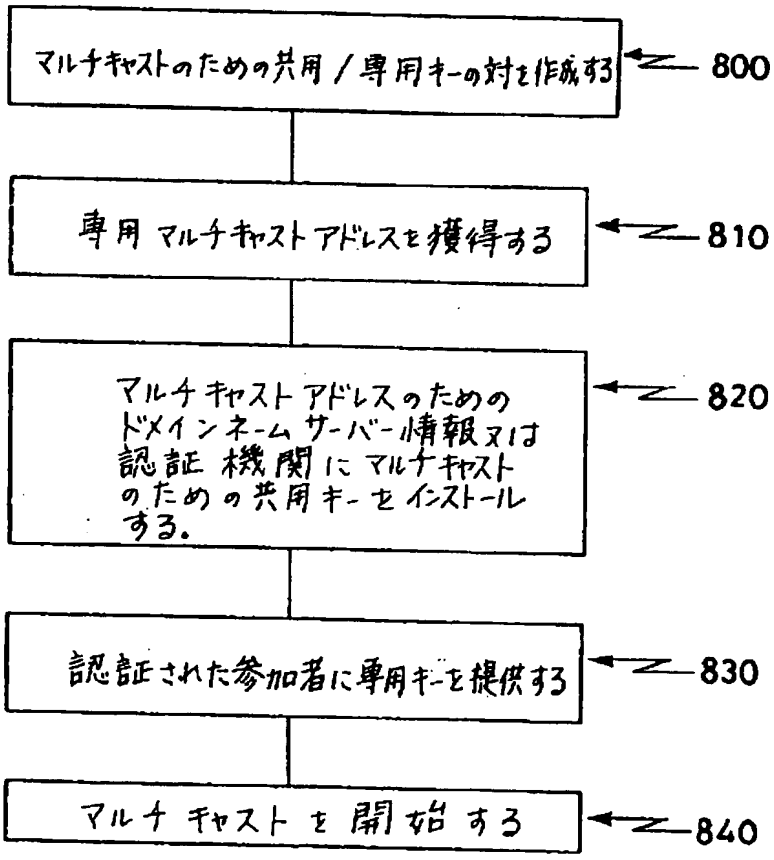
【図５】



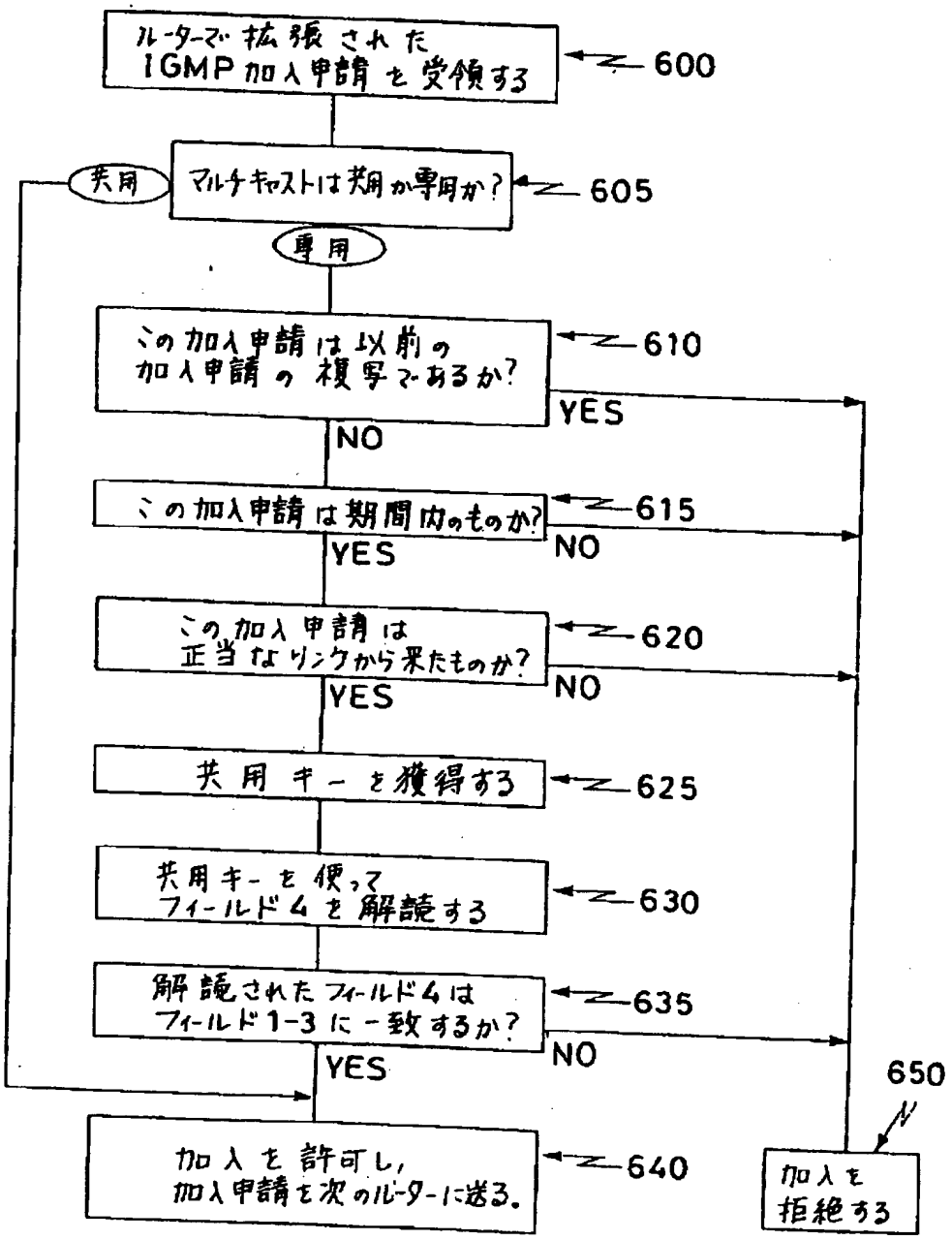
【図4】


400
410
420
430
440
ネットワークアドレス
別名
所有者
共用キー
任意の共用/専用フラグ
221.0.96.3
MULTICAST.hostsponsor.com
abc123@hostsponsor.com
AXJY931ZFDE271...KJ
1

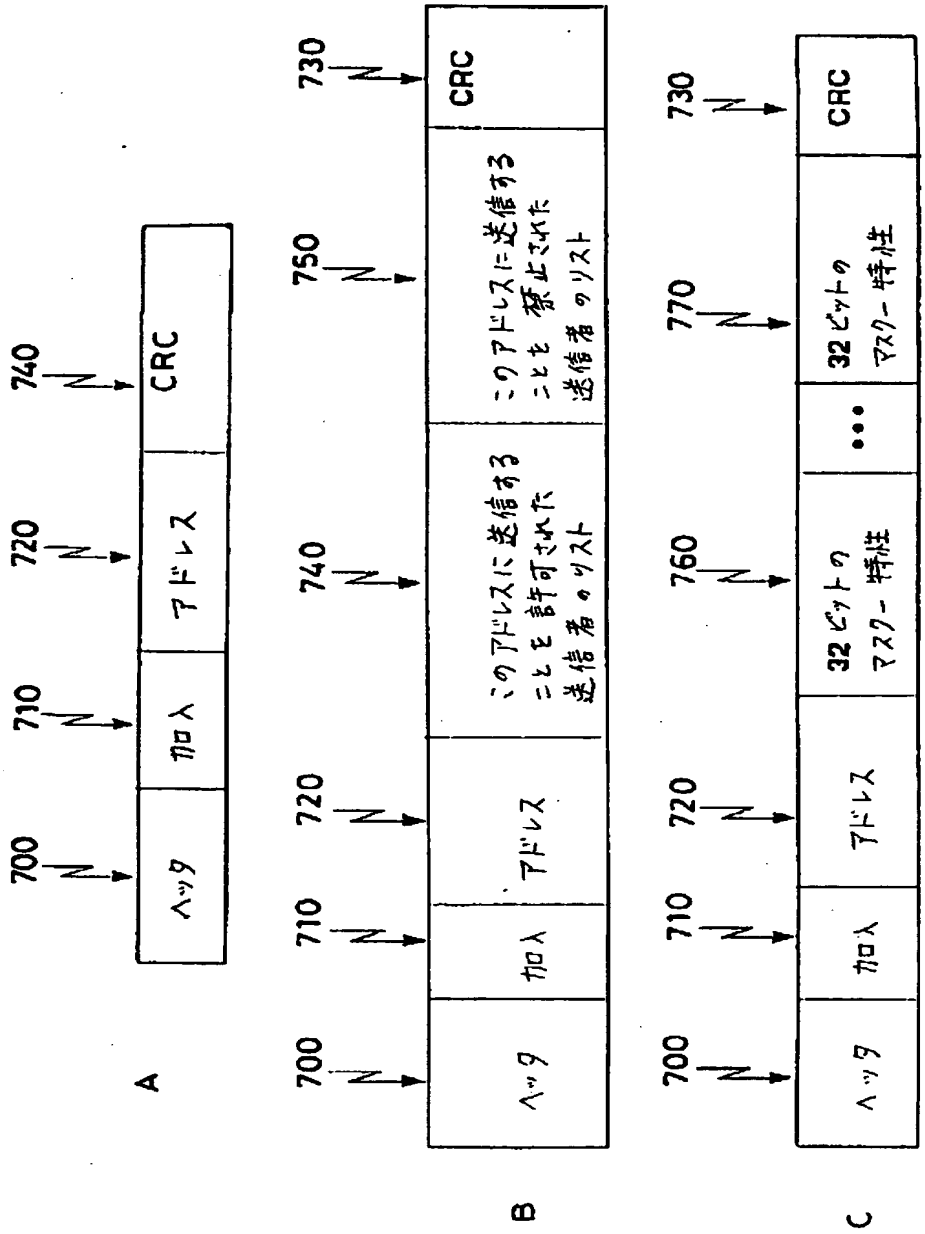
【図8】


マルチキャストのための共用/専用キーの対を作成する
800
専用マルチキャストアドレスを獲得する
810
マルチキャストアドレスのためのドメインネームサーバー情報又は認証機関にマルチキャストのための共用キーをインストールする。
820
認証された参加者に専用キーを提供する
830
マルチキャストを開始する
840

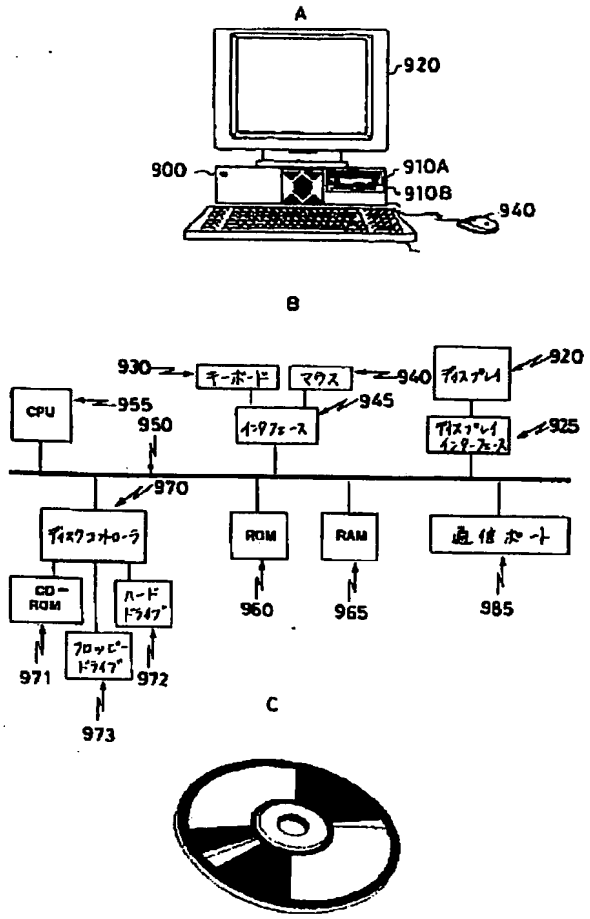
【図6】


ルーターで拡張された IGMP加入申請を受領する
600
共用
マルチキャストは共用か専用か?
605
専用
この加入申請は以前の加入申請の複写であるか?
610
YES
NO
この加入申請は期間内のものか?
615
YES
NO
この加入申請は正当なリンクから来たものか?
620
YES
NO
共用キーを獲得する
625
共用キーを使ってフィールド4を解読する
630
解読されたフィールド4はフィールド1-3に一致するか?
635
YES
NO
加入を許可し,加入申請を次のルーターに送る。
640
加入を拒絶する
650

【図7】


A
700
710
720
740
ヘッダ
加入
アドレス
CRC
B
700
710
720
740
750
730
ヘッダ
加入
アドレス
この アドレスに 送信する ことを 許可された 送信者 のリスト
この アドレスに 送信する ことを 禁止された 送信者 のリスト
CRC
C
700
710
720
760
770
730
ヘッダ
加入
アドレス
32 ビットの マスク 特性
•••
32 ビットの マスク 特性
CRC

【図９】



フロントページの続き

(71)出願人　591064003
901　SAN　ANTONIO　ROAD
PALO　ALTO，CA　94303，U.
S．A.

(72)発明者　ポール　ダブリュー．ジャーデツキー
アメリカ合衆国、カリフォルニア　94305、
スタンフォード、カサノバ　プレース
950

【外国語明細書】

TECHNIQUES FOR SECURING DATA FLOW IN INTERNET MULTICASTING

BACKGROUND OF THE INVENTION

Field of the Invention

The invention relates to telecommunications systems and more particularly to securing data flow in Internet multicasting.

Description of Related Art

Many emerging Internet applications involve one-to-many or many-to-many communications, where one or multiple sources are sending to multiple receivers. Examples are the transmission of corporate messages to employees, communication of stock quotes to brokers, video and audio conferencing for remote meetings and telecommuting, and replicating databases and web site information. IP Multicast efficiently supports this type of transmission by enabling sources to send a single copy of message to multiple recipients who explicitly want to

receive the information. This is far more efficient than requiring the source to send an individual copy of the message to each requester (referred to as point-to-point *unicast*), in which case the number of receivers is limited by the bandwidth available to the sender. It is also more efficient than broadcasting one copy of the message to all nodes (*broadcast*) on the network, since many nodes may not want the message, and because broadcasts are limited to a single subnet.

IP Multicasting is a receiver-based concept: a receiver joins a particular multicast session group and traffic is delivered to all members of that group by the network infrastructure. The sender does not need to maintain a list of receivers. Only one copy of a multicast message will pass over any link in the network, and copies of the message will be made only where paths diverge at a router. Thus multicast yields many performance improvements and conserves bandwidth end-to-end.

IP Multicasting is described in more detail in two documents published by the IP Multicast Initiative. The first is entitled "How IP Multicast Works" and the second is entitled "Introduction to IP Multicast Routing". These documents are attached to the specification as Appendixes A and B, respectively. These documents are

hereby incorporated by reference into the specification in their entirety.

A related approach to multicast security using encryption of datastreams is known in which a sender encrypts outgoing information for decryption at a receiver. This is commonly done using public key encryption techniques.

The Problems

IP Multicasting is based on a simple design -- the sender simply sends the data to a multicast group address and the network automatically sends the data to everyone who expressed interest in receiving data on that multicast address. A significant problem is that this arrangement does not provide any security to data flow, that is, everyone can listen to a multicast session and everyone can send data to multicast sessions. As a result, there is no such thing as secure data flow in Internet multicasting sessions in the prior art. Further, since anyone can send to a multicast session, the potential for disruption by an interloper is significant.

SUMMARY OF THE INVENTION

Various aspects of the invention discussed herein provide apparatus, systems, processes, and computer

program products for securing data flow in Internet Multicasting. This is done by splitting the multicast address space into two components, one for public multicast and one for private multicast. A public key of a public/private pair is installed on a domain name server or on a certification authority and is associated with the multicast address. A user, desiring to join a private multicast, provides certain information which is encrypted using the private key of the public/private key pair. Routing functions are typically performed by a switch at a node of a switching network or by a router in the network or by a computer which has a plurality of communications interfaces. As used herein, the term "routing element" applies to all. A routing element receives a join request, obtains the public key and compares some non-encrypted information with decrypted information for consistency. The routing element also performs certain other checks on the join request received. Only when the routing element is satisfied that the join request received is authentic does the routing element permit the join and forward the join request to the next routing element on the way to the source. Techniques are also provided for source-group specific joins and leaves which permit one to specify senders authorized to send to a receiver and to prevent unauthorized senders from sending data to the receiver.

One embodiment of the invention is directed to a routing element for routing multicast information. The routing element obtains a public key with which to decode part of a multicast join request to verify that a user is authorized to join a private multicast.

Another embodiment of the invention is directed to apparatus for participating in a multicast including a processor configured to send a private multicast join request.

Another embodiment of the invention is directed to a domain name server which stores records relating a multicast network address or alias with a public key of a public/private key encryption pair and which sends in response to a network address or alias received over a communications port, a public key corresponding to the address or alias.

Another embodiment of the invention is directed to a communications system for multicasting information from at least one source to a plurality of receivers, including a plurality of sub-networks and at least one router, connecting at least two sub-networks, configured to distinguish between public and private multicasts.

Another embodiment of the invention relates to a method of operating a communications system by providing a multicast address space having a subspace for public multicasts and a subspace for private multicasts.

Another embodiment of the invention relates to a method of sending a multicast join request, by sending first information including a user identification and an optional random key together with an encrypted version of said first information.

Another embodiment of the invention relates to a method of sending a multicast join request from a user by sending a list of bit-masks specifying at least one of a group of senders permitted to send to said user and a group of senders prohibited from sending to said user.

Another embodiment of the invention relates to a method of establishing a private multicast by creating a private/public key encryption pair, distributing private keys to authorized participants in the multicast; obtaining a private multicast address; and installing the public key for the multicast on a domain name server or on a certification authority.

Other embodiments of the invention relate to computer program products for carrying out the techniques described.

The foregoing and other features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings and Appendices A and B of this specification.

BRIEF DESCRIPTION OF DRAWINGS

The objects, features and advantages of the system of the present invention will be apparent from the following description in which:

Figure 1 is block diagram of an exemplary network arrangement linking a plurality of sub-networks in accordance with one aspect of the invention.

Figure 2 is a illustration of how a multicast address space may be partitioned into a private multicast address sub-space and public multicast address sub-space, in accordance with one aspect of the invention.

Figure 3 is a database schema showing a typical domain name server record in accordance with the prior art.

Figure 4 is a database schema of a domain name server modified in accordance with one aspect of the invention.

Figure 5 is a diagram illustrating the extensions to an Internet Group Management Protocol (IGMP) join request in accordance with one aspect of the invention.

Figure 6 is a flow chart of an exemplary router process for determining whether to permit or reject an IGMP join request in accordance with one aspect of the invention.

Figure 7A shows a prior art IGMP join request.

Figure 7B shows a prior art extension to the IGMP join request of Figure 7A.

Figure 7C shows an extension to IGMP join requests in accordance with one aspect of the invention.

Figure 8 is a flow chart of a process for setting up a private multicast in accordance with one aspect of the invention.

Figure 9A illustrates a computer of a type suitable for carrying out the invention.

Figure 9B illustrates a block diagram of the computer of Figure 9A.

Figure 9C illustrates an exemplary memory medium containing one or more programs usable with the computer of Figure 9A.

NOTATIONS AND NOMENCLATURE

The detailed descriptions which follow may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are the means used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art.

A procedure is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those requiring physical manipulations of physical quantities. Usually, though

not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

Further, the manipulations performed are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein which form part of the present invention; the operations are machine operations. Useful machines for performing the operation of the present invention include general purpose digital computers or similar devices.

The present invention also relates to apparatus for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a general purpose computer as selectively activated or reconfigured by a computer program stored in the computer. The procedures presented herein are not

inherently related to a particular computer or other apparatus. Various general purpose machines may be used with programs written in accordance with the teachings herein, or it may prove more convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 is a block diagram of an exemplary network arrangement linking a plurality of sub-networks in accordance with one aspect of the invention. As shown in **Figure 1**, a plurality of sub-networks **100A**, **100B**, **100C** and **100D** are connected together over routers **110A**, **110B** and **110C**. In the network illustrated, domain name server **130** is resident on sub-network **100B** and a certification server or authority **150** as resident on sub-network **100C**. One or more senders **140** may be the intended source of information for the multicast to exemplary user stations 120A and 120B.

Figure 2 is an illustration of how a multicast address space may be partitioned into a private multicast address sub-space and public multicast address sub-space.

The left hand side of **Figure 2** represents the total multicast address space. That space ranges from

224.0.0.0 (in Internet standard dotted decimal notation) to 239.255.255.255. Underneath the dotted decimal representation is a parenthetical showing eight binary bits (bracketed) which corresponds to the numerical value of the first component of the dotted decimal notation). Each of the other components of the dotted decimal notation represent the value of a corresponding byte in a 32-bit (4 byte) address space utilized by the Internet. The notation of a binary value 1 or 0 separated by dots from another representation of the same binary value represents an indication that the remaining bits of the 32-bit address word have only those binary values contained therein. One of the important extensions to the multicast address space provided in accordance with the invention is a separation of the multicast address space into two components, the first of which is a public multicast address space and the second of which is a private multicast address space. As shown in Figure 2, the public multicast address space ranges from 224.0.0.0 to 231.255.255.255. Similarly the private multicast address space ranges from 232.0.0.0 to 239.255.255.255. By this partitioning of the address space, one can tell immediately from a multicast address whether a private multicast is undertaken or a public multicast is undertaken.

Figure 3 is a database schema showing a typical domain named server (DNS) record in accordance with the prior art. As shown in Figure 3, a dotted decimal address 300 is mapped against an alias for that address 310 in respective columns of the database table.

Figure 4 is a database schema of a domain name server modified in accordance with one aspect of the invention. Columns 400 and 410 correspond to approximately to the columns in which entries 300 and 310 of Figure 3 occur. However, in column 410, instead of a fixed station address, an IP Multicast address is included. Column 420 contains entries which describe the owner of the multicast address. Typically this would be the person setting up the multicast. Column 430 contains a public key for each private multicast address. Column 440 contains an optional public or private flag which can be used to distinguish public and private multicasts if the address space is not partitioned.

When using a domain name server of the prior art, a query using either the network address or it alias will result in return of the other value shown in Figure 3. When a domain name server is extended in accordance with the arrangement shown in Figure 4, it is convenient that a query submitted with data from either column 400 or column 410 will result in return of the entire record matching the submitted value. Thus, if one were to

search on the alias shown in column 410 of Figure 4, one would retrieve not only the network address shown in column 400, the owner information shown in 420 but also the public key shown in column 430 for the multicast session. This ability to retrieve public keys is useful as described more in after.

Figure 5 is a diagram of extension to an Internet Group Management Protocol (IGMP) join request in accordance with one aspect of the invention. A header 500, and packet type shown in Field 1 together with a requester IP address shown in Field 2 would typically be part of prior art IGMP join request. In the extensions shown in accordance with one aspect of the invention, an optional timestamp may be placed in Field 1 and a random key, placed in Field 3, is generated by the requestor. The contents of Field 1, Field 2 and Field 3 are encrypted or digested and the digest encrypted and placed into Field 4. The Cyclic Redundancy Check 510 (CRC) encompasses the full IGMP join request. How this extended join request is utilized is discussed more hereinafter.

Figure 6 is a flow chart of an exemplary routing element process for determining whether to permit or reject an IGMP join request in accordance with one aspect of the invention. When an extended IGMP join request is received at a router (600) determination is made from the address whether or not the multicast is public or private

(605). If it is public (605-public), the join is permitted and the join request forwarded to the next routing element along the path, if any (640). If the multicast is private (605-private) a check is made to determine whether the join request submitted is a duplicate of a previous request. One way an unauthorized user may attempt to gain access to a multicast would be to duplicate a join request submitted by a previous user. If the submitted join request is a duplicate (610-y), the request is rejected. If it is not, a determination is made whether the join request is timely (615). This a simple check to see that the join request is appropriate for the day and time of the current multicast session. This would prevent a user from copying an earlier join request from an authorized user in an attempt to gain access to the current session. If the join request is not timely (615-N), the request to join is rejected. If it is timely, a check is made to determine whether the join request came from a proper link. If it did not (620-N), the join request is rejected. However, if it did, the routing element will obtain the public key dual corresponding to the private key utilized to encrypt the IGMP extended join request (625). Preferably, the public key is obtained from a domain name server, such as DNS 130 shown in **Figure 1**. Alternatively, the public key could be obtained from a certification authority 150

shown in **Figure 1**. Using the acquired public key, Field 4 of the extended IGMP join request is decrypted using the public key (630). The resulting information decrypted from Field 4 should agree with Fields 1-3. If it does, the join is permitted and the join request is forwarded to the next routing element. If it does not (635-n), the join request is rejected and the user will be denied access to the multicast by the router.

A third aspect of the invention is illustrated in **Figure 7A**, **Figure 7B** and **Figure 7C**. **Figure 7A** shows a prior art IGMP join request.

Figure 7B shows a prior art extension to the IGMP join request of **Figure 7A**. The extension of the IGMP join request of **Figure 7B** permits a lists of senders to be specified which are permitted to send to the address requesting the join. Similarly, it includes an list of senders prohibited from sending to the address requesting the join. This permits a participant in the multicast to inform routers to selectively prohibit packets from undesirable or disruptive sources from reaching the participant. It also permits the user to specify the list of senders from which the requesting station desires to receive information. This allows the filtering out of packets that the user does not desire to see.

Figure 7C shows an extension to prior art IGMP join requests in accordance with one aspect of the invention.

Field 760 and Field 770 permit the use of a list of 32-bit masks instead of a list of senders or receivers. Thus, by tailoring a mask, groups of addresses may be permitted to send to the address or barred from sending to the address, merely by specifying the bit-mask appropriate for the group and the property desired. For example, the property may be "permitted to send to this address" or "prohibited from sending to this address".

Figure 8 is a flow chart of a process for setting up a private multicast in accordance with one aspect of the invention. A user desiring to set up a private multicast first creates a private/public key pair for the multicast (800). The sponsor or owner of the multicast obtains a private multicast address (810) for use during the multicast. This can either be a permanent assignment or a temporary assignment depending on need. The owner of the multicast or other designated party may install the public key for the multicast in the DNS information for the multicast address or in a certification server (820). The private key for the multicast is distributed to authorized participants in any of several known ways, but preferably over the network (810). At that time, the multicast is ready to begin (840). The receivers that desire to participate in the multicast then formulate an extended join request such as described in Figure 5. If the user is authorized, the routing element will make

that determination using the public key installed on the domain named server or on the certification server. When the routing element is satisfied that the request for joining the private multicast is genuine, the routing element will begin directing packets addressed to the multicast address to the user who submitted in the extended IGMP join request. However, if the user is not authorized (as discussed in conjunction with **Figure 6**), the user will not be permitted to join the multicast and the routing element will not forward packets to the user.

Figure 9A illustrates a computer of a type suitable for carrying out the invention. Viewed externally in **Figure 9A**, a computer system has a central processing unit **900** having disk drives **910A** and **910B**. Disk drive indications **910A** and **910B** are merely symbolic of a number of disk drives which might be accommodated by the computer system. Typically, these would include a floppy disk drive such as **910A**, a hard disk drive (not shown externally) and a CD ROM drive indicated by slot **910B**. The number and type of drives varies, typically, with different computer configurations. The computer has the display **920** upon which information is displayed. A keyboard **930** and a mouse **940** are typically also available as input devices. Preferably, the computer illustrated in **Figure 9A** is a SPARC workstation from Sun Microsystems, Inc.

Figure 9B illustrates a block diagram of the internal hardware of the computer of **Figure 9A**. A bus **950** serves as the main information highway interconnecting the other components of the computer. CPU **955** is the central processing unit of the system, performing calculations and logic operations required to execute programs. Read only memory (**960**) and random access memory (**965**) constitute the main memory of the computer. Disk controller **970** interfaces one or more disk drives to the system bus **950**. These disk drives may be floppy disk drives, such as **973**, internal or external hard drives, such as **972**, or CD ROM or DVD (Digital Video Disks) drives such as **971**. A display interface **975** interfaces a display **920** and permits information from the bus to be viewed on the display. Communications with external devices can occur over communications port **985**.

Computer **900** includes a communications interface **985** coupled to bus **950**. Communications interface **985** provides a two-way data communications coupling to a network link to a local network such as **100D** of **Figure 1**. For example, if communications interface **985** is an integrated services digital network (ISDN) card or a modem, communications interface **985** provides a data communications connection to the corresponding type of telephone line. If communications interface **985** is a local area network (LAN) card, communications interface

985 provides a data communications connection to a compatible LAN. Wireless links are also possible. In any such implementation, communications interface 985 sends and receives electrical, electromagnetic or optical signals which carry digital data streams representing various types of information.

The network link typically provides data communications through one or more networks such as 100A-110D of Figure 1, to other data devices. For example, the network link may provide a connection through local network to a host computer or to data equipment operated by an Internet Service Provider (ISP). An ISP may in turn provide data communications services through the world wide packet data communications network now commonly referred to as the "Internet". The local network and Internet both use electrical, electromagnetic or optical signals which carry digital data streams. The signals through the various networks and the signals on the network link and through communications interface 985, which carry the digital data to and from computer 900 are exemplary forms of carrier waves transporting the information.

Computer 900 can send messages and receive data, including program code, through the network(s), network link and communications interface 985. In the Internet example, a server might transmit requested code for an

application program through Internet, ISP, local network and communications interface 986. In accordance with the invention, one such download application may include software implementing the techniques described herein.

The received code may be executed by processor 955 as it is received, and/or stored in storage devices 960 and/or 971-973, or other non-volatile storage for later execution. In this manner computer 900 may obtain application code in the form of a carrier wave.

Figure 9 shows an architecture which is suited for either a user workstation or for a routing element. However, when configured as a routing element, I/O devices will normally only be attached during servicing. When configured as a router, a plurality of communications interfaces 985 will normally be provided, one for each port. When configured as a controller for a switch at a switching node, a hardware interface will be provided to link the bus 950 with a switching matrix.

Figure 9C illustrates an exemplary memory medium which can be used with drives such as 973 in Figure 9B or 910A in Figure 9A. Typically, memory media such as a floppy disk, or a CD ROM, or a Digital Video Disk will contain the program information for controlling the computer to enable the computer to perform its functions in accordance with the invention.

The approach discussed above provides a simple general purpose interface that works across a spectrum of varying user needs. It does not unreasonability increase the overhead for setting up and operating the multicast for users who would like to continue to set up simple open meetings. The systems provides security even if outsiders know the IP address and/or port number which might otherwise enable them to misbehave or behave maliciously. The system is flexible in that it does not require the multicast sessions organizers to know the identity of all the senders and/or listeners in advance. It also permits users to dynamically join the discussions.

Even if the system is compromised, it is possible to reasonably limit the damage caused by excluding that user or group of users from the conference. The approach described here is also compatible with current and proposed mechanism and protocols for multicasting.

Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation, the spirit and scope of the present invention being limited only by the terms of the appended claims and their equivalents.

What is claimed is:

1. A routing element for multicast digital communications, comprising:

a. at least one input port;

b. at least one output port;

c. a processor for controlling packet routing from an input port to an output port, said processor configured to obtain a public key and to decode at least a portion of a multicast join request submitted by a user using said public key to verify that said user is authorized to join a multicast.

2. The routing element of claim 1 in which said public key is obtained from a domain name server.

3. The routing element of claim 1 in which said public key is obtained from a certification authority.

4. The routing element of claim 1 which blocks multicast packets from a particular multicast to said user, unless the decoding of the multicast join request submitted by said user indicates said user is authorized to join said particular multicast.

5. The routing element of claim 1 in which the processor is configured to obtain a public key only when a multicast join request specifies a multicast address which is within a private multicast address space.

6. The routing element of claim 1 in which the processor is configured to block multicast packets received from senders blocked from sending to a receiver as indicated by a bit-mask received with a multicast join request.

7. Apparatus for participating in a multicast, comprising:

a. a communications port;

b. a processor for controlling communications over said communications port; said processor configured to send a private multicast join request.

8. Apparatus of claim 7 in which said multicast join request includes a first field identifying a user requesting participation in a particular multicast and a second field containing the results of encrypting at least one of said first field or a digest of said first field using a private key.

9. Apparatus of claim 7 in which said second field contains the results of encrypting one of said first field and a third field containing a randomly generated key or a digest of said first field and said third field.

10. Apparatus of claim 7 in which said join request includes at least one bit-mask, a bit-mask specifying one of a group of senders permitted to send to said communications port and a group of senders prohibited to send to said communications port.

11. A domain name server comprising:

a. a communications port;

b. a memory storing records relating a network address or alias for a multicast with a corresponding public key of a public/private key encryption pair; and

c. a processor controlling said communications port; said processor being configured to send, in response to a network address or alias received over said communications port, said corresponding public key.

12. The server of claim 11 in which said records include an indication of an owner of a multicast.

13. The server of claim 11 in which said records include an indication distinguishing whether a multicast is public or private.

14. A communications system for multicasting information from at least one source to a plurality of receivers, comprising:

a. a plurality of sub-networks, each having at least one user device connected thereto; and

b. at least one routing element, connecting at least two sub-networks, configured to distinguish between public and private multicasts.

15. The system of claim 13, further comprising: a domain name server, connected to a sub-network, storing records relating a network address or alias with a public key of a public/private key encryption pair.

16. The system of claim 13, further comprising: a certification authority, connected to a sub-network, storing records relating a network address or alias with a public key of a public/private key encryption pair.

17. The system of claim 13 in which a user device is configured to request participation in a private multicast.

18. A method of operating a communications system comprising the step of:

providing a multicast address space having a subspace for public multicasts and a subspace for private multicasts.

19. A method of sending a multicast join request, comprising the step of:

a. sending first information including a user identification together with an encrypted version of said first information.

20. The method of claim 18 in which said first information further includes a random key.

21. A method of sending a multicast join request from a user, comprising the step of:

a. sending a list of bit-masks specifying at least one of a group of senders permitted to send to said user and a group of senders prohibited from sending to said user.

22. A method of processing a multicast join request at a router, comprising the step of:

a. determining whether the request relates to a public or private multicast.

23. The method of claim 21, further comprising the steps of:

a. obtaining a public key and using the public key to decrypt at least a portion of said request.

24. The method of claim 22, further comprising, the step of granting said multicast join request when a decrypted portion of said request matches another portion of said request.

25. A method of establishing a private multicast, comprising the steps of:

a. creating a private/public key encryption pair;

b. distributing private keys to authorized participants in the multicast;

c. obtaining a private multicast address; and

d. installing the public key for the multicast on a domain name server or on a certification authority.

26. A computer program product, comprising:

a. a memory medium; and

b. a computer program stored on said memory medium, said computer program comprising instructions for

providing a multicast address space having a subspace for public multicasts and a subspace for private multicasts.

27. The computer program product of claim 25 in which said program is transmitted from said memory medium over a network interface.

28. A computer program product, comprising:

a. a memory medium; and

b. a computer program stored on said memory medium, said computer program comprising instructions for sending a multicast join request, including a user identification together with an encrypted version of said user identification.

29. The computer program product of claim 27 in which said program is transmitted from said memory medium over a network interface.

30. A computer program product, comprising:

a. a memory medium; and

b. a computer program stored on said memory medium, said computer program comprising instructions for sending a group specific multicast join including a bit-mask specifying at least one of a group of senders permitted

to send to said user and a group of senders prohibited from sending to said user.

31. The computer program product of claim 29 in which said program transmitted from said memory medium over a network interface.

32. A computer program product, comprising:

a. a memory medium; and

b. a computer program stored on said memory medium, said computer program comprising instructions for determining whether the request relates to a public or private multicast and for obtaining a public key and using the public key to decrypt at least a portion of said request.

33. The computer program product of claim 31 in which said program is transmitted from said memory medium over a network interface.

34. A computer program product, comprising:

a. a memory medium; and

b. a computer program stored on said memory medium, said computer program comprising instructions for creating a private/public key encryption pair; obtaining a private multicast address; and installing the public

key for the multicast on a domain name server or on a certification authority.

35. The computer program product of claim 33 in which said program is transmitted from said memory medium over a network interface.

36. A computer data signal embodied in a carrier wave and representing a sequence of instructions which, when executed by one or more processors, causes the one or more processors to obtain a public key and decode at least a portion of a multicast join request submitted by a user using said public key.

37. A memory for storing data for access by an application program being executed on a computer, comprising:

a data structure stored in memory, said data structure comprising an IGMP join request, a requestor IP address and an encrypted version of at least part of information contained in the IGMP join request and said requestor IP address.

38. A memory for storing data for access by a server program being executed on a computer, comprising:

a data structure stored in memory, said data structure including a plurality of entries, each entry including a multicast address and an indication whether the multicast address is a public or a private multicast.

39. The memory of claim 38 in which data structure entries include a location for storage of a public key.

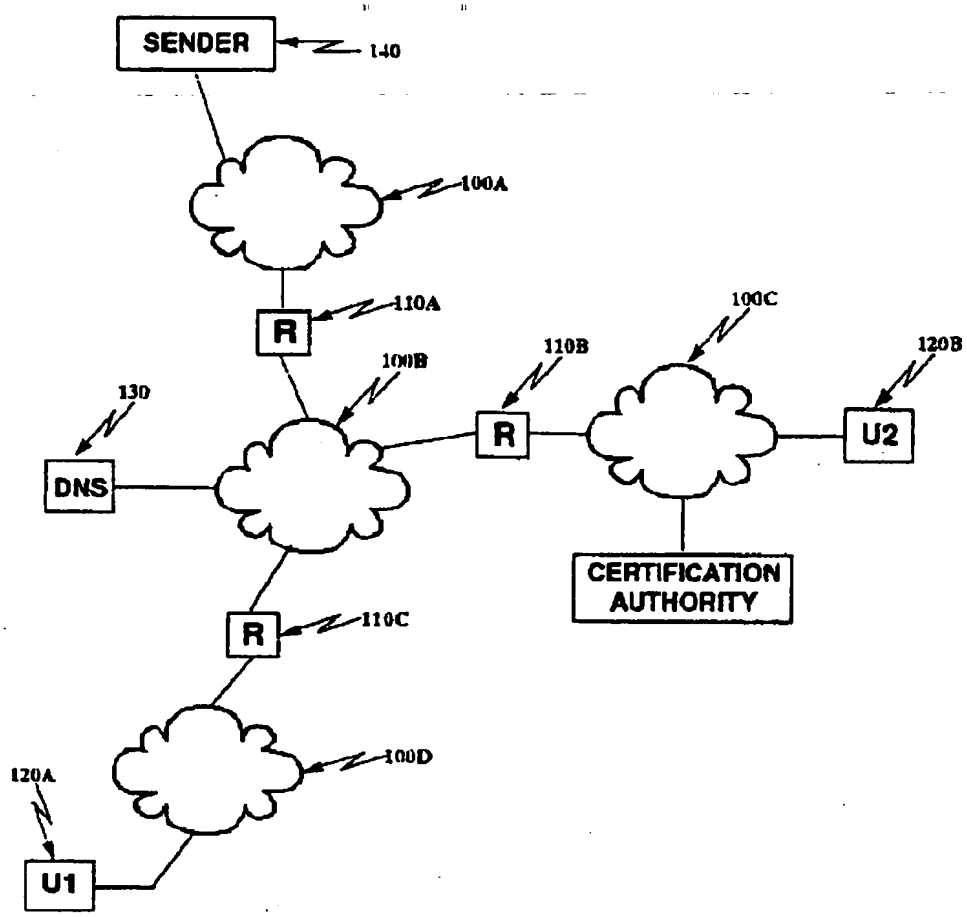

SENDER
140
100A
110A
R
100C
110B
120B
130
100B
R
U2
DNS
CERTIFICATION AUTHORITY
R
110C
100D
120A
U1

Figure 1

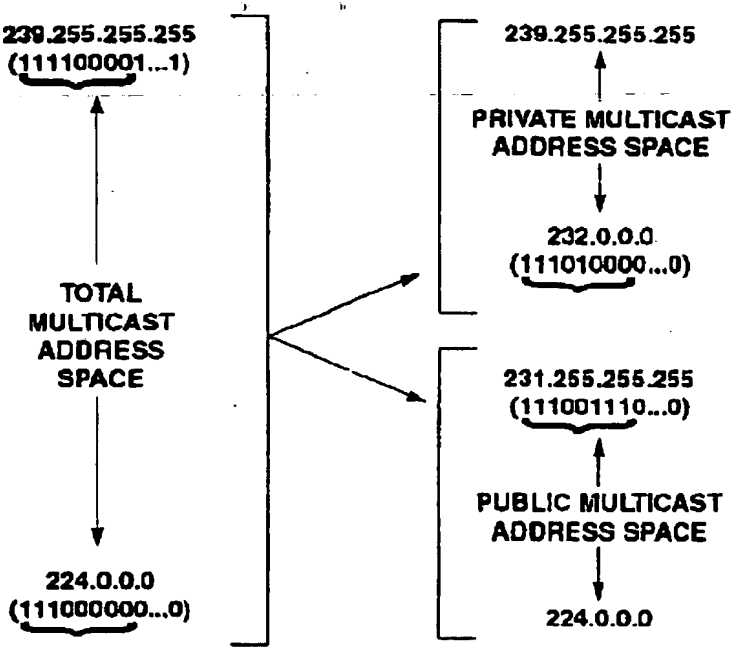


Figure 2

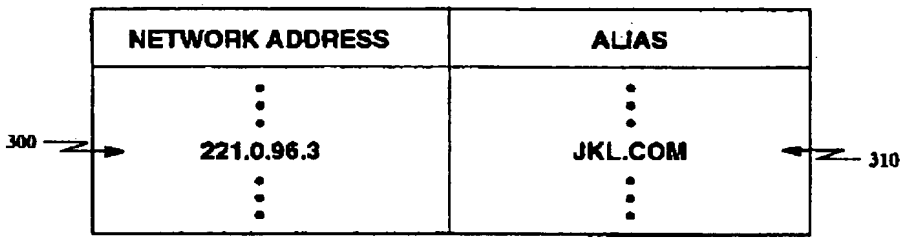


Figure 3

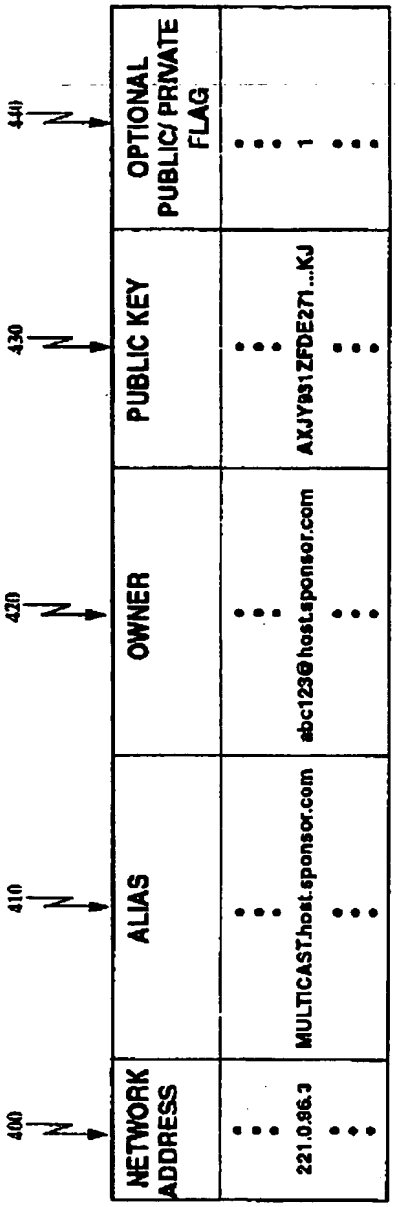


Figure 4

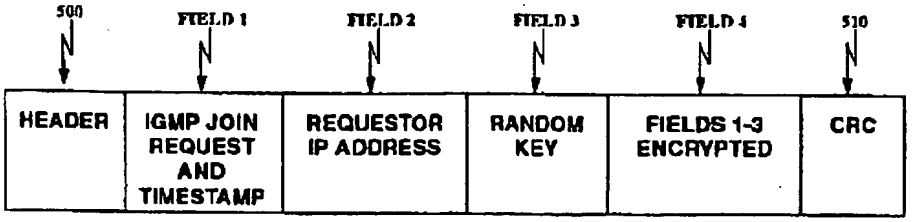


Figure 5

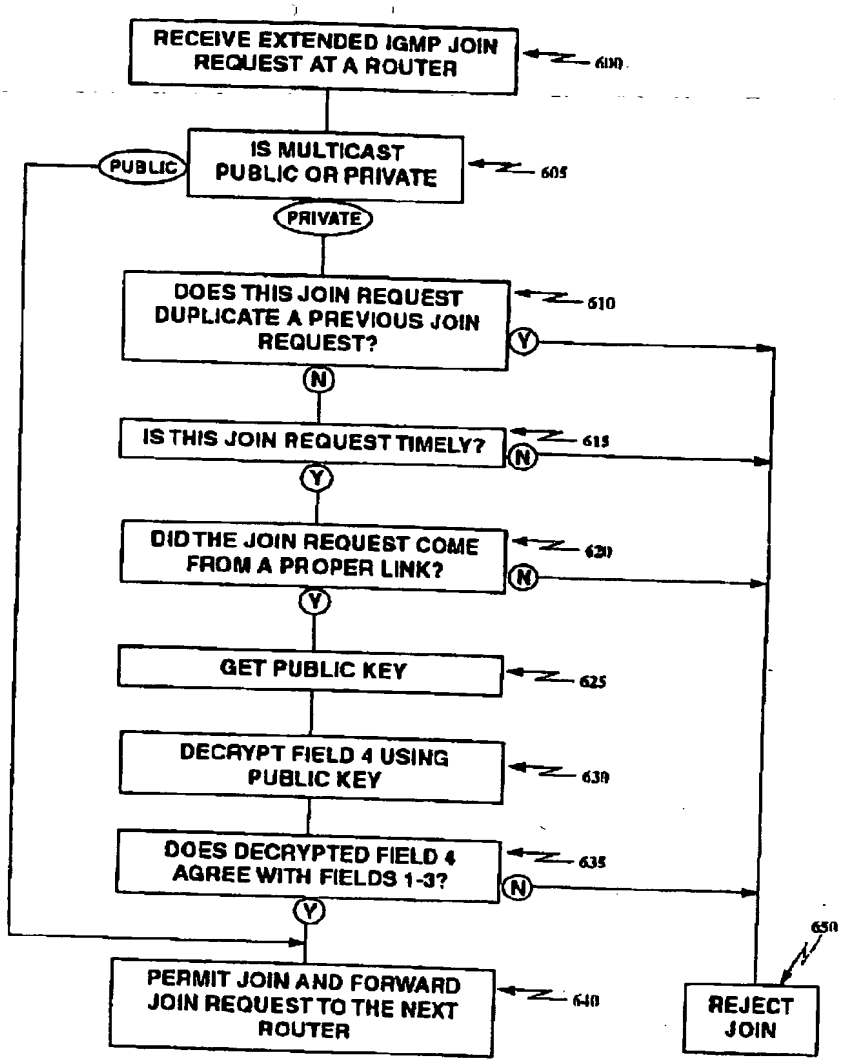

RECEIVE EXTENDED IGMP JOIN REQUEST AT A ROUTER
600
IS MULTICAST PUBLIC OR PRIVATE
605
PUBLIC
PRIVATE
DOES THIS JOIN REQUEST DUPLICATE A PREVIOUS JOIN REQUEST?
610
Y
N
IS THIS JOIN REQUEST TIMELY?
615
N
Y
DID THE JOIN REQUEST COME FROM A PROPER LINK?
620
N
Y
GET PUBLIC KEY
625
DECRYPT FIELD 4 USING PUBLIC KEY
630
DOES DECRYPTED FIELD 4 AGREE WITH FIELDS 1-3?
635
N
Y
PERMIT JOIN AND FORWARD JOIN REQUEST TO THE NEXT ROUTER
640
REJECT JOIN
650

Figure 6

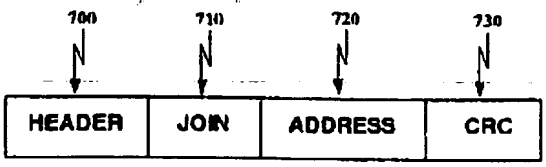


Figure 7A

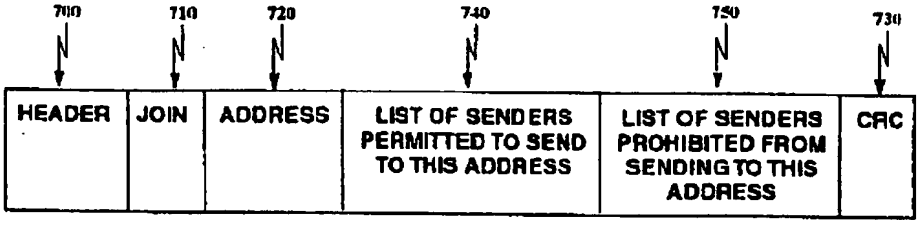


Figure 7B

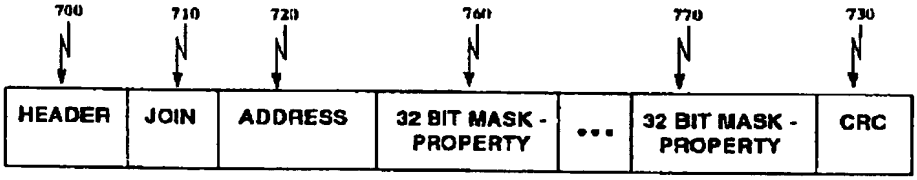


Figure 7C

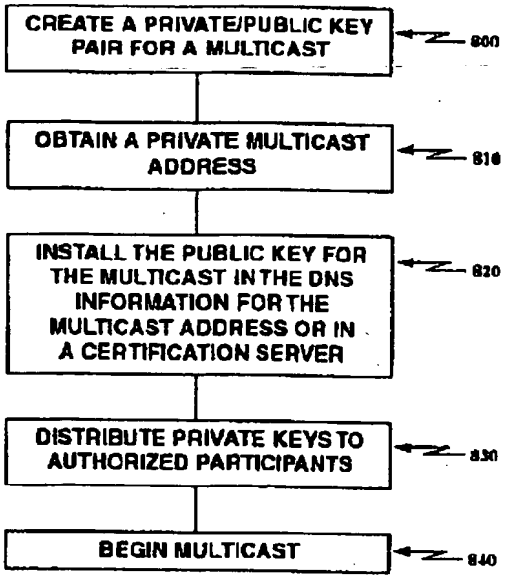

CREATE A PRIVATE/PUBLIC KEY PAIR FOR A MULTICAST
800
OBTAIN A PRIVATE MULTICAST ADDRESS
810
INSTALL THE PUBLIC KEY FOR THE MULTICAST IN THE DNS INFORMATION FOR THE MULTICAST ADDRESS OR IN A CERTIFICATION SERVER
820
DISTRIBUTE PRIVATE KEYS TO AUTHORIZED PARTICIPANTS
830
BEGIN MULTICAST
840

Figure 8

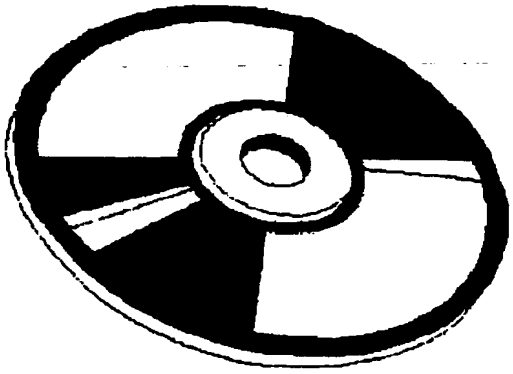


Figure 9C

Multicast communications are expanded to include the concept of private multicasts. An address space dedicated to multicast is partitioned into a subspace for public multicasts and a subspace for private multicasts. A public key/private key encryption pair is used for private multicasts and installed on domain name servers or on certification authorities. Portions of a multicast join request are sent together with a corresponding encrypted version. Private multicast equipped routers receive the multicast join request, retrieve the public key from a domain name server or from a certification authority and decrypt the encrypted portion of the join request to determine if the requestor is authorized. Group specific multicast joins are also permitted by sending a bit-mask identifying a group of senders which are authorized or prohibited from sending to a user joining a multicast.